PCT/GB98 / 0 3 7 5 6

GB 98/03756

09/367396

EJV

Europäisches Patentamt
European Patent Office
Office européen des brevets

REC'D 08 JAN 1999
WIPO PCT

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

98304246.6

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

H.I. Block

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE 27/07/98

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 98304246.6
Demande n°:

Anmeldetag:
Date of filing: 29/05/98
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
Hewlett-Packard Company
Palo Alto, California 94304
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Monitoring ISDN links

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	EP	Tag: Date: Date:	15/12/97	Aktenzeichen: File no. Numéro de dépôt:	EPA97310155

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/CY
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

Monitoring ISDN links

[30980016-2]

Technical Field

This invention relates to monitoring systems which collect data from an Integrated Services Digital Network (ISDN).

Background

The Integrated Services Digital Network has been designed to provide customers with digital access to the public network, which can carry a number of different services at a range of different bandwidths. The narrowband ISDN is extensively deployed worldwide. The broadband ISDN is in early deployment and trial phases with a number of operators. The network that operators will actually have to manage will be a combination of existing digital and analogue networks, narrowband ISDN, broadband ISDN, internet technology and other technologies. A specific service is likely to use resources from a number of these different networks (Figure 2 shows some examples of the resources and technologies involved). This presents major problems in the end-to-end management of the service. The monitoring system described here addresses many of these problems.

Disclosure of Invention

According to one aspect of this invention there is provided a method of monitoring an ISDN link, comprising the steps of: monitoring at a first location subscriber signalling messages on an ISDN D channel to derive first monitoring data; monitoring at said first location telecommunications traffic traversing ISDN B channels associated with said ISDN D channel to derive second monitoring data; and correlating said first and second monitoring data.

In some case it may be desirable to monitor additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network (such as the public switched telephone network – PSTN) coupled to said ISDN link, to derive third monitoring data, and correlate those third monitoring data with at least one of the first and second monitoring data. Another option is to monitor signalling messages and telecommunications traffic on ISDN links at a second location, and correlate the resulting monitoring data with those first and second monitoring data.

According to another aspect of this invention there is provided a method of monitoring an ISDN link, comprising the steps of: monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data; monitoring additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network coupled to said ISDN link, to derive second monitoring data; and correlating said first and second monitoring data.

According to a further aspect of this invention there is provided apparatus for monitoring an ISDN link, comprising: first equipment at a first location for monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data; second equipment at said first location for monitoring telecommunications traffic traversing ISDN B channels associated with said ISDN D channel to derive second monitoring data; and correlation apparatus coupled to said first and second equipment to receive and correlate said first and second monitoring data.

According to another aspect of this invention there is provided apparatus for monitoring an ISDN link, comprising the steps of: first equipment for monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data; second equipment for monitoring additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network coupled to said ISDN link, to derive second monitoring data; and correlation apparatus coupled to said first and second equipment to receive and correlate said first and second monitoring data.

Brief Description of Drawings

Methods and apparatus in accordance with this invention for monitoring ISDN links will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows a distributed ISDN monitoring system;

Figure 2 shows examples of local loop and core network probe measurements which may be correlated to create end-to-end service records; and

Figure 3 shows one exemplary architecture for combined monitoring of an ISDN and an SS7 signalling system.

Best Mode for Carrying Out the Invention, & Industrial Applicability

The distributed monitoring system shown in the drawings has the capability to collect data from an ISDN, correlate these data in real-time, and provide a real-time view of services on the network. These data can be used for applications such as troubleshooting, surveillance, security, network planning, provision of accounting information to customers, fraud detection, billing and marketing information. The monitoring system can be used to monitor multiple ISDNs which may be interconnected by other technologies, such as internet protocol (IP) networks. Part of the ISDNs may be made up of older technologies, such as analogue.

Referring to Figure 1, the probes shown are part of a distributed monitoring system, and may be implemented as either link monitoring devices (using techniques similar to those in existing protocol analysers for example) or as software and hardware on network elements (such as nodes and switches). The distributed monitoring system is constructed from the probes and standard computer and communications components, with specialised software which provides the applications described above. A principal function of this specialised software is to correlate data from different probes to provide a record or real-time trace of calls, transactions and other services as they occur on the network. The Hewlett-Packard *acceSS7* system is an example of a distributed monitoring system which could be used to implement parts of the system described above.

According to this invention monitoring of the local loop is also provided, in respect of subscriber signalling and the services themselves (for example the content of the B channels of primary rate access (PRA) or basic rate access (BRA) ISDN); furthermore data from any of the probes covering any of the technologies in the local loop or core network (see Figure 2) may be correlated (e.g. data from a probe for any local loop protocol at one end of the service, plus data from a probe for any core network protocol, plus data from a probe for any local loop protocol at the other end of the service).

An example of a monitoring system architecture is given in Figure 3. This shows probes monitoring both the SS7 network and the PRA ISDN. The SS7 probes could be for example from the Hewlett-Packard *acceSS7* system. The ISDN primary rate access probes could for example be constructed using the same techniques as in existing protocol analysers (such as the Hewlett-Packard 37900D Signalling Test Set).

According to this invention the distributed monitoring system is arranged to correlate real-time data from any combination of these probes. This includes, for example, the D channel and B channel of ISDN PRA and the signalling units from SS7.

The invention can be applied in respect of other protocols and technologies in the access network. An important example is the use of remote digital terminals to concentrate a number of different local loop technologies to a common interface. The local loop technologies supported are: traditional analogue connections, ISDN primary rate and basic rate, various copper-pair based high-speed digital subscriber loop technologies (e.g. ADSL, HDSL), "Fibre in the Loop" and wireless technologies. The ITU-T V5 specification and the Bellcore GR-303 series of specifications are examples of architectures used to concentrate the subscriber loop technologies. Probes can be constructed which monitor the connection between the digital terminal and the local switch (e.g. the V5 or GR-303 protocol), using technologies already available for protocol analyser products such as the HP 37900D. The probes can determine the signalling protocol on the connection, and monitor the bearer channels, in a similar way to the ISDN monitoring architecture shown in Figure 3. This data source should be considered part of the distributed monitoring system for the following discussion. Service usage data can be obtained from this source in a similar way as for ISDN, but for a broader range of subscriber loop technologies.

For convenience the invention is described primarily with reference to narrowband ISDN and its associated B (bearer) channels and D (data) channel. However, it should be understood that this terminology is to be taken as including within its scope channels with analogous functionality in broadband ISDN systems, whether or not they are customarily identified by these terms.

GENERATION OF SERVICE RECORDS

This section lists the types of fields in service records, and describes how the distributed monitoring system could provide the required data. A service record is generated for each instance of the usage of a specific service. This is a generalisation of a call record, which is generated by current switches. A service is normally defined from the perspective of the user. The service may actually involve a number of calls or transactions, for example. The service records described here correlate together these different calls and transactions, using information from the SS7 and ISDN signalling information, to provide a single record of the service.

1. Calling Party Information.

This includes any information which can be derived about the calling party from the data flowing on the links of the Integrated Services Digital Network, and is therefore available to the link monitoring probes. Typical information includes: calling party number; any ISDN sub-addressing information; calling party name; X.25 or frame relay addresses; other network addresses; and any numbers or addresses related to billing.

This information may be derived from: call setup messages on the ISDN D channels, at either the originating or terminating end or both; and/or from call setup messages on any of the SS7 links. Additional information may be derived from the ISDN B channel for certain services such as frame relay. In this case the headers of the frames contain addressing information. Additional information may also be derived from any intelligent network services messages which flow over the SS7 links as part of the specific service usage. Further information may be derived from looking at the ISDN B or D channels of any intelligent peripherals involved in the specific service usage.

2. Called Party Information.

As for calling party information, but replace calling party by called party.

3. Network Routing Information.

This may include any information on the network resources which were used to provide this specific service usage. The following are examples of data which might be provided:

- ISDN links and channels used;
- SS7 links and nodes used;
- trunks used;
- intelligent network nodes used.

Each of these uses is time-stamped, and the sequence and nature of the use indicated.

These data can be obtained in a similar way as was described for item 1 above.

4. Intelligent Network Services Information.

This may include any information on intelligent network services used for this specific service usage. The following are some examples of the data which may be provided:

- calling party name delivery information;
- local number portability information;
- call forwarding information;
- interactive voice response information on the use of intelligent peripherals;
- 800 number services.

This information includes time-stamps, duration and the nature of the use.

These data can be obtained in a similar way as was described for item 1 above.

5. Service Status and Termination Information.

This may include time-stamped information on the initiation of the service, any status changes occurring during service and the termination of the service. The termination information should include the reasons for termination.

These data can be obtained in a similar way as was described for item 1 above. In particular, the call clearing messages on the SS7 links and the ISDN D channels can provide details on the reasons for call termination.

6. Analysis of B-Channel to Distinguish Voice from Fax or Data.

As part of the process of generating service records, the B-channel associated with a particular call can be identified from the signalling messages on the corresponding D-channel. The probe monitoring the link carrying the B-channel can be instructed to capture data from the B-channel. An analysis of the spectrum of this captured data can be used to identify the type of service being carried in the B-channel. This could be used for distinguishing a voice call from a fax or data call. The probe can be instructed to periodically sample the B-channel to check for any change in the type of service being used.

7. Analysis of Tones in the B-Channel to Identify Any Additional Dialled Data.

The probe may also be instructed to analyse the data captured from the B-channel to identify any multi-frequency tones (eg DTMF) which may provide further information about the call. This may be used to identify any additional digits dialled by the subscriber after the initial call is connected. These digits can be added to any service record which is generated by the monitoring system for the call. It could also used for identifying a fax call from the signalling between two fax machines.

8. Service Type.

This may include information on the following types of services:

- voice;
- modem;
- fax;
- video;
- X.25;
- frame relay;
- ATM (asynchronous transfer mode);
- LAN interconnection.

These data can be obtained in a similar way as was described for item 1 above. In particular, the call establishment messages in the ISDN D channel provide information on the type of service. This can be correlated with data taken from the ISDN B channels identified in the ISDN D channel signalling.

9. Service Quality Information.

The service quality information provided is dependent on the service indicated in the service type field. The following gives some examples of what can be provided for specific services.

Voice quality is mainly indicated by the bit error rate and the delay. These parameters can be measured using a passive monitoring system, by using the signalling information to identify the ISDN B channels which are carrying the voice signals. The bit streams from each of the B channels identified can be compared to derive the delay and bit error rate caused by the intermediate networks. This is particularly important where one of the intermediate networks is packet or frame based and cannot guarantee delivery times (e.g. IP protocol or ATM).

Video, modem and fax quality can be addressed in a similar way.

The data oriented protocols (X.25, frame relay, ATM and LAN interconnection) require additional data. These can again be measured by using SS7 or ISDN signalling data from the probes to identify the ISDN channels carrying the protocol. Existing protocol analysis techniques can be used to provide estimates of parameters like packet loss, retransmissions, CRC errors, throughput and packet delay.

10. Service Usage Information.

The time of usage data provided by the distributed monitoring system depends on the specific service. Some examples follow.

Voice, video and fax services require call duration and allocated bandwidth.

The data oriented services require data such as total bits, frames and packets in each direction. This may be provided for regular time intervals for the duration of the service. It may also be broken down into a traffic matrix, where the data protocol has additional addressing information (such as IP addresses). The data are obtained in a similar way as is described for item 9 above.

11. Security Information.

A particular instance of service usage may be an attempt to obtain unauthorised access to resources. The service record includes information which may indicate this type of behaviour. This may include information about the duration of call, the way the call was terminated and details of the service used.

An example would be where a modem is used repeatedly to try different passwords. The ISDN B channel used is identified from SS7 and ISDN signalling data. The probes then extract the data from the ISDN B channel, and the system can determine the modem protocol to identify behaviour.

The examples described above focus mainly on narrow band ISDN. However the same concepts apply to broadband ISDN and ATM. Variants of the Q.931 protocol are used in these standards for users to network interface signalling (UNI) and network to network interface signalling (NNI). These can be monitored in a similar fashion, and service records generated from the sequence of messages which control a particular call. The concept of channels is replaced by the concepts of virtual paths and virtual channels. However, the virtual path and virtual channel associated with a particular call can be identified from the signalling messages, and the probes monitoring the links which carry these virtual paths and channels can be instructed to capture the data associated with the call and provides an analysis similar to the narrow band case for inclusion in the service record which is generated.

REAL-TIME UPDATES ON SERVICE USE

The data that populates the service records described in the previous section is collected in real-time from the monitoring probes. These data can be provided in real-time on remotely connected computers as they becomes available. A user of the distributed monitoring system can apply filtering criteria on any of the information described in the previous section, to select those instances of service use for which real-time updates are required.

APPLICATIONS

The following applications can be implemented using the data from the service records described above or the real-time service updates. Data from other sources may be used to enhance the effectiveness of these applications.

A. Quality of Service and Service Level Agreements.

The service records described above can be used to provide service quality information on selected customer's service. This can be used to track conformance to service level agreements, and be provided to the customer as an additional service. It can be provided as periodic reports, or in real-time using the real-time updates described above.

B. Surveillance and Troubleshooting for Network Operations.

The service records and real-time updates can be used to identify service or network faults. The information can also be used to troubleshoot the faults.

C. Fraud Detection.

The service records and real-time updates can be used to identify potential fraudulent use of the network or service. Indications may include excessive use of high value services, unusual call termination behaviour and repeated failures to gain access to a service. The distributed monitoring system may be used to track the service usage of potential high-risk users in real-time.

D. Security and Hacking Detection

Potential security threats can be identified by repeated failures to gain access to a service. They also may be indicated by successful access to sensitive services, such as

maintenance ports on customer premises equipment (CPE). This type of data is available from the service records and the real-time updates.

E. Billing Data

The service records can be used as a basis for billing which is dependent on any of the fields in the service record. This allows, for example, billing to be based on the actual service quality delivered. It also enables billing to reflect the nature and generation of the usage of resources on the network, such as intelligent peripherals and databases.

F. Use of B-Channel Data for Billing or Billing Verification Purposes.

In some countries the regulatory requirements for Telecom operators require that calls carrying voice have a different tariff to calls carrying data. They also require that any access charges between operators depend on whether the call is voice or data, and if it is voice there is also a dependency on the final destination for call. The service records generated by the monitoring system can be used to determine the bill in these cases (and similar situations), using the data derived from the B-channel as described in respect of items 6 and 7 above.

G. Customer Accounting Data

The detailed service usage information in the service records can be provided to customers for use in their internal accounting. This includes the traffic matrix information for packet and frame based protocols, which the system derives from the B and D ISDN channels.

H. Customer and Telecom Operator Network Planning

The service records can provide detailed information on the use of network resources which can be provided to network planning departments within the operator and the customer.

SS7 SIGNALLING NETWORKS AND VOICE TRUNK NETWORKS

1. A Monitoring System to Provide Call Records Containing Data from Both the SS7 Signalling Network and the Trunk Network.

A monitoring system such as Hewlett-Packard's *acceSS7* system can be used to generate call (or service) records by monitoring the sequences of messages on the SS7

network. This monitoring system can be extended with probes which monitor the trunks which carry the voice path for calls. The trunk carrying the voice path for a particular call can be identified from fields with in the SS7 messages (normally the TCIC in the IAM). The probe connected to this trunk can then be instructed to capture the data from the trunk for analysis in real-time or at a later date.

2. Analysis of "Voice Path" to Distinguish Voice from Fax or Data.

As part of the process of generating service records, the trunk associated with a particular call can be identified from the signalling messages on the corresponding SS7 network. The probe monitoring the trunk can be instructed to capture data from the trunk. An analysis of the spectrum of this captured data can be used to identify the type of service being carried in the call. This could be used for distinguishing a voice call from a fax or data call. The probe can be instructed to periodically sample the trunk to check for any change in the type of service being used.

3. Analysis of Tones in the "Voice Path" to Identify Any Additional Dialled Data.

The probe may also be instructed to analyse the data captured from the trunk to identify any multi-frequency tones (eg DTMF) which may provide further information about the call. This may be used to identify any additional digits dialled by the subscriber after the initial call is connected. These digits can be added to any service record which is generated by the monitoring system for the call. It could also used for identifying a fax call from the signalling between two fax machines.

4. Use of "Voice Path" Data for Billing Purposes.

In some countries the regulatory requirements for Telecom operators require that calls carrying voice have a different tariff to calls carrying data. They also require that any access charges between operators depend on whether the call is voice or data, and if it is voice there is also a dependency on the final destination for call. The service records generated by the monitoring system can be used to determine the bill in these cases (and similar situations), using the data derived from the "Voice Path" as described above.

CLAIMS

[30980016-2]

1. A method of monitoring an ISDN link, comprising the steps of:

monitoring at a first location subscriber signalling messages on an ISDN D channel to derive first monitoring data;

monitoring at said first location telecommunications traffic traversing ISDN B channels associated with said ISDN D channel to derive second monitoring data; and

correlating said first and second monitoring data.

2. A method according to claim 1, including the steps of:

monitoring additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network coupled to said ISDN link, to derive third monitoring data; and

correlating said third monitoring data with at least one of said first and second monitoring data.

3. A method according to claim 1, including the steps of:

monitoring at a second location subscriber signalling messages on an ISDN D channel to derive fourth monitoring data;

monitoring at said second location telecommunications traffic traversing ISDN B channels associated with said ISDN D channel to derive fifth monitoring data; and

correlating said fourth and fifth monitoring data with said first and second monitoring data.

4. A method of monitoring an ISDN link, comprising the steps of:

monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data;

monitoring additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network coupled to said ISDN link, to derive second monitoring data; and

correlating said first and second monitoring data.

5. Apparatus for monitoring an ISDN link, comprising:

first equipment at a first location for monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data;

second equipment at said first location for monitoring telecommunications traffic traversing ISDN B channels associated with said ISDN D channel to derive second monitoring data; and

correlation apparatus coupled to said first and second equipment to receive and correlate said first and second monitoring data.

6. Apparatus for monitoring an ISDN link, comprising:

first equipment for monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data;

second equipment for monitoring additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network coupled to said ISDN link, to derive second monitoring data; and

correlation apparatus coupled to said first and second equipment to receive and correlate said first and second monitoring data.

7. A method of monitoring a telecommunications system having transmission channels and an associated signalling channel, comprising the steps of:

monitoring at a first location signalling messages on the signalling channel to derive first monitoring data;

selecting a transmission channel identified by reference to information contained in said first monitoring data;

monitoring at said first location telecommunications traffic traversing the selected transmission channel to derive second monitoring data; and

extracting further information traversing the selected transmission channel by reference to information contained in said second monitoring data.

8. The method of claim 7, wherein the transmission channel is an ISDN B channel and the signalling channel is an ISDN D channel.

9. The method of claim 7, wherein the transmission channel is carried by a telephone transmission link and the signalling channel is carried by a common channel signalling link, such as an SS7 signlling link.

10. The method of any one of claims 7 to 9, wherein said further information comprises dual-tone multi-frequency (DTMF) signals.

ABSTRACT

Monitoring ISDN links

[30980016]

Telecommunications signals (voice and/or data) are provided to a subscriber via B channels of an Integrated Services Digital Network (ISDN) link coupled to a public switched telephone network (PSTN) incorporating an SS7 signalling system. A monitoring system extracts data from subscriber signalling messages traversing the ISDN link's D channel and from messages traversing the SS7 signalling system, and generates additional monitoring data by measuring parameters of the telecommunications signals on the B channels. These data are correlated to derive information to assist management of telecommunications services provided via the ISDN link.

(Fig. 3)

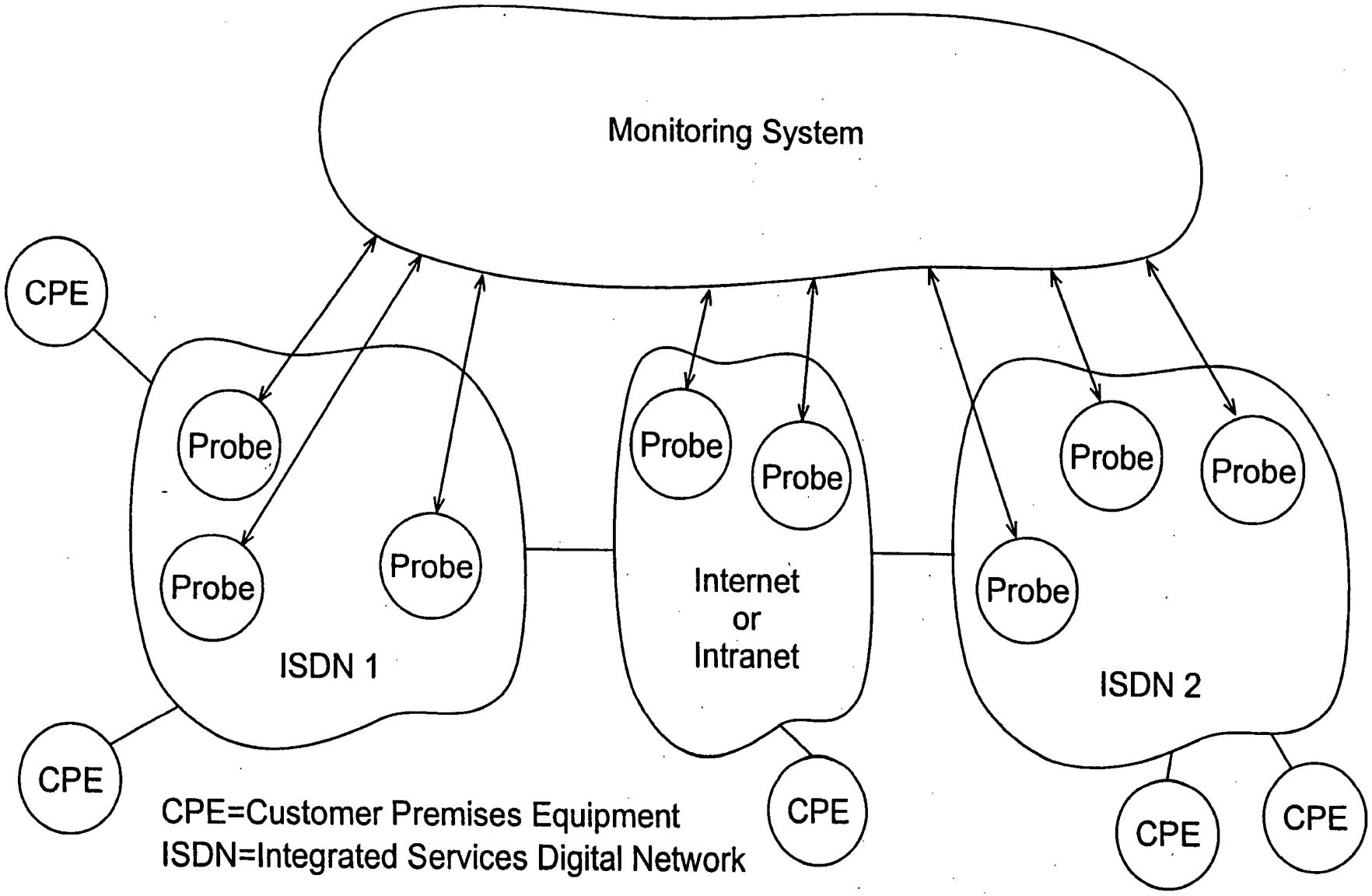

Fig.1: ISDN Distributed Monitoring System

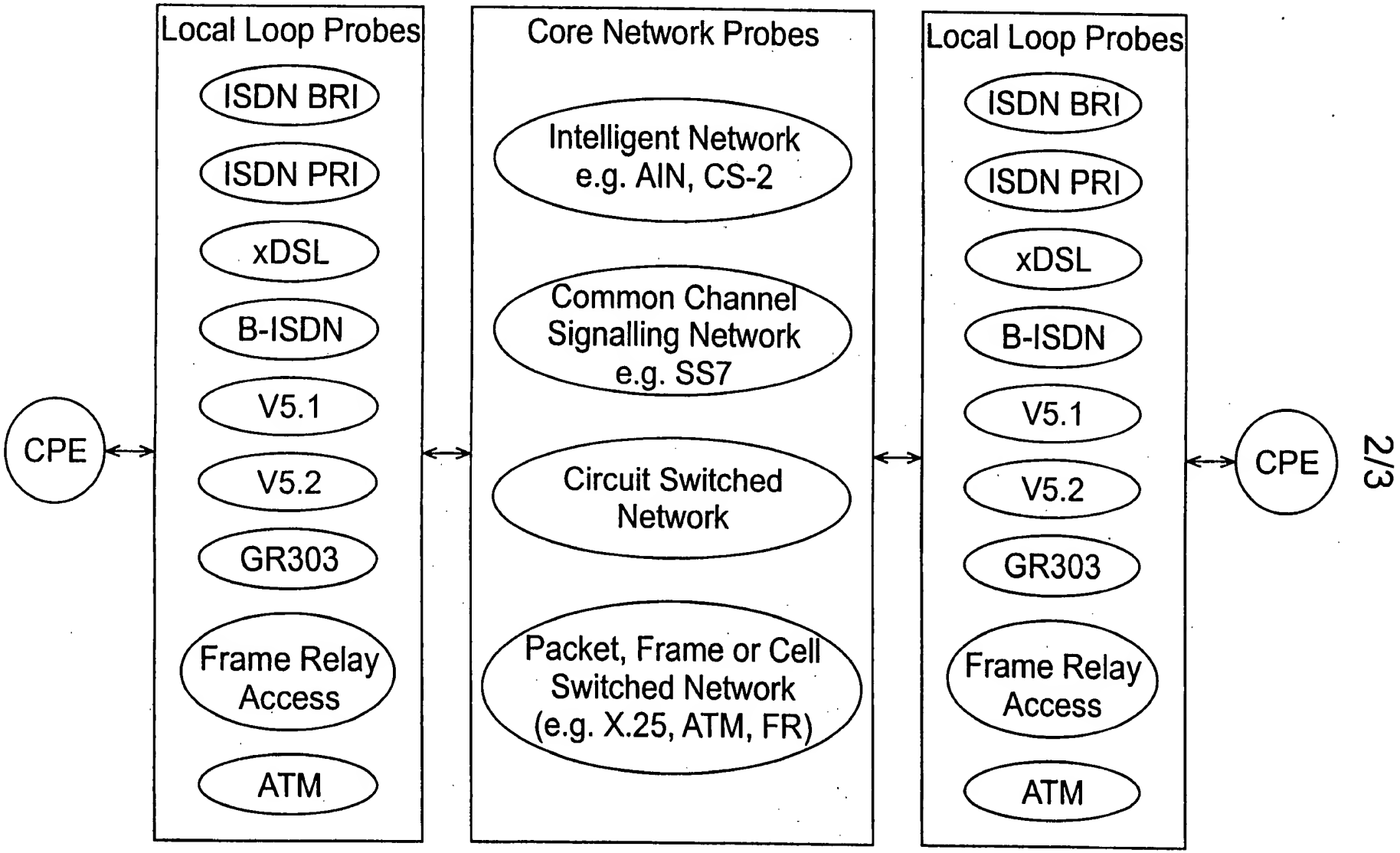

Fig.2: Correlation of local loop monitoring probes with core network monitoring probes to provide end-to-end service records

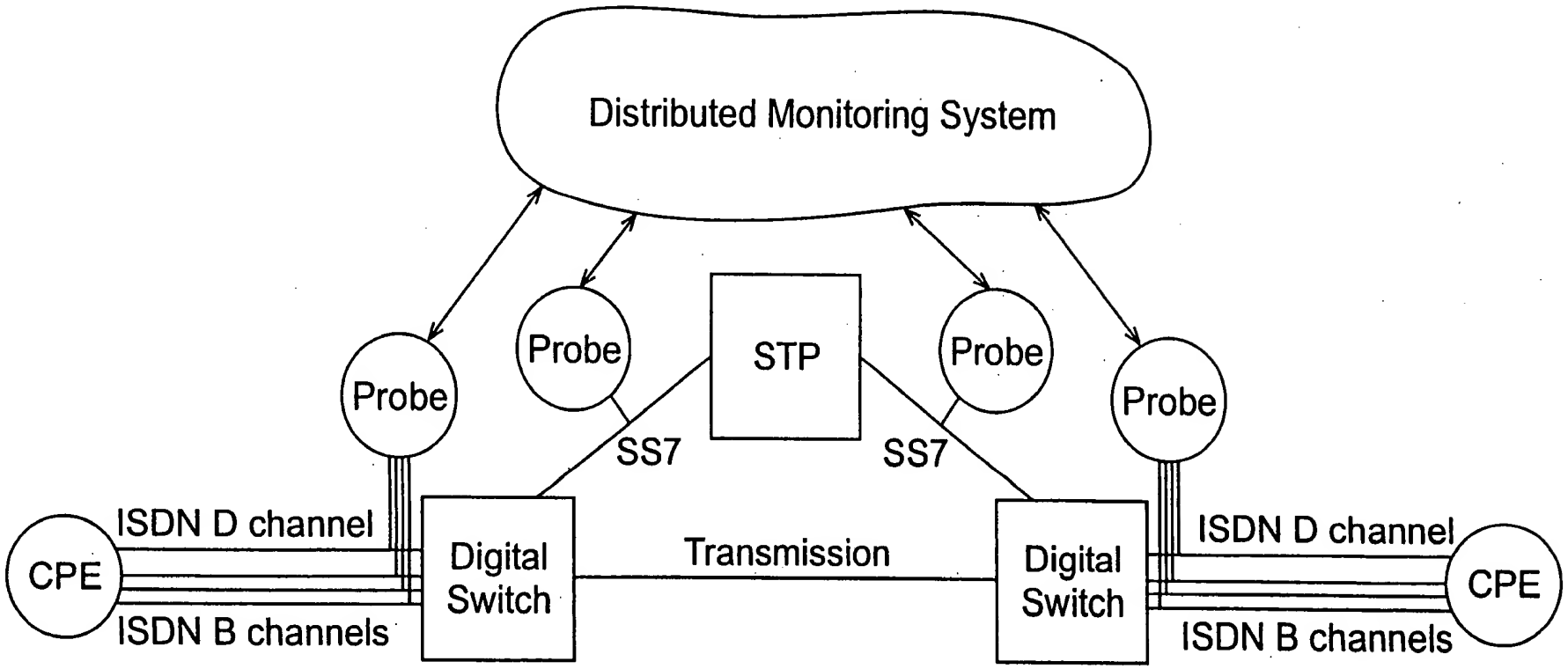

Fig.3: Example of Architecture for Monitoring ISDN and SS7 Networks

THIS PAGE BLANK (USPTO)